Topics of Interest

Iraklion, Greece
June 2008

Kim Davies
Internet Assigned Numbers Authority

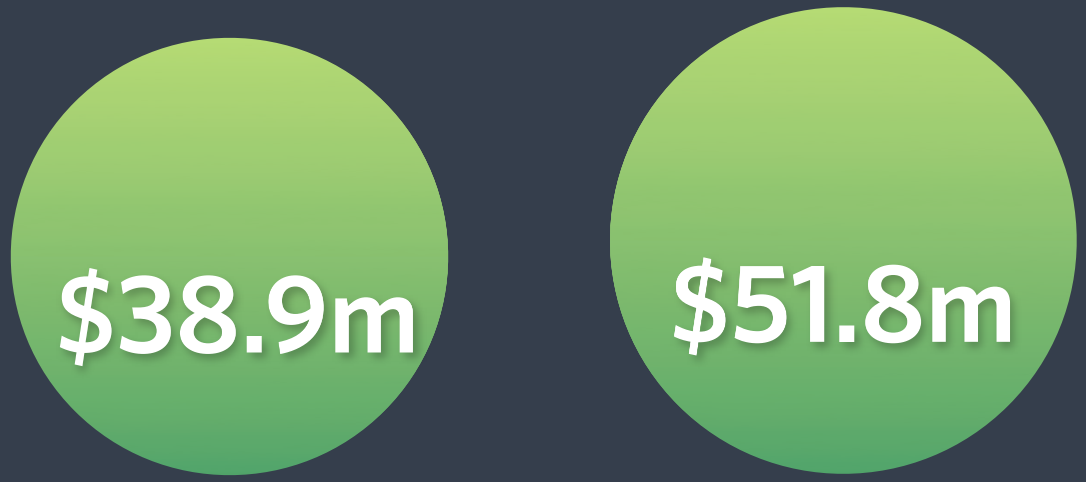
Agenda

- ICANN Budget for 2009
- Interim Trust Anchor Repository
- Process for implementation of RZM software
- Root server “hijacking”

ICANN Budget for Fiscal Year 2009

Total ICANN Operating Expenses

FY08 → FY09



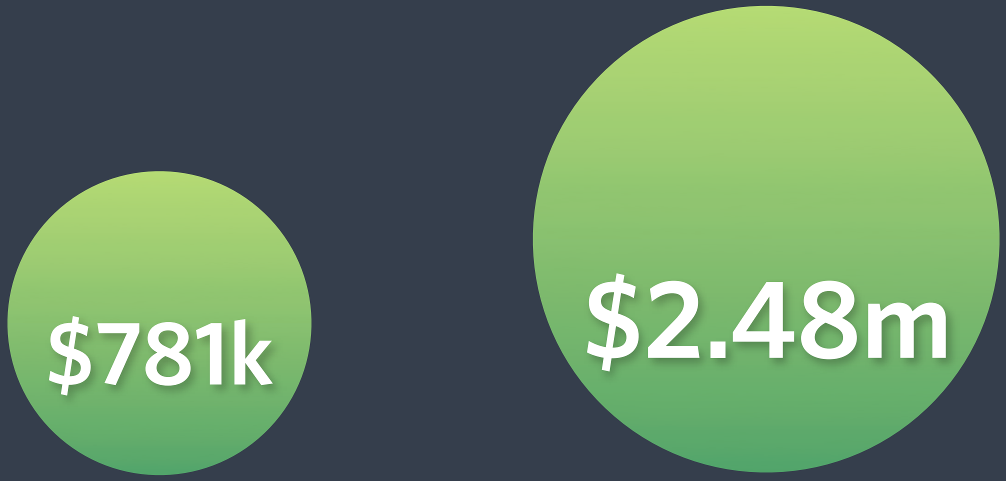
$38.9m

$51.8m

+33%

“Strengthening IANA and Infrastructure”

FY08 → FY09



+218%

140
120
100
80

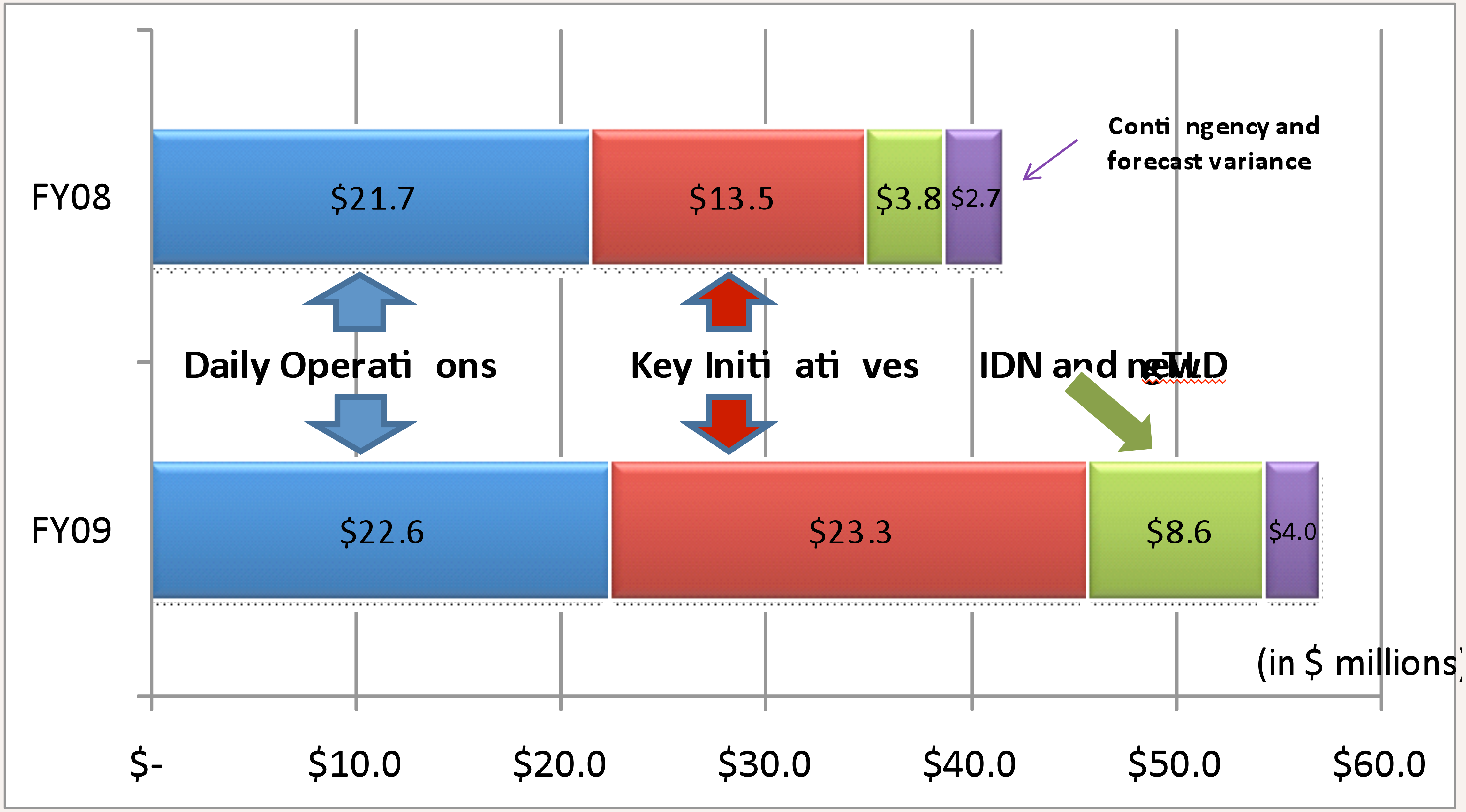
???

“Strengthening IANA and Infrastructure”

- Redundancy and Business Continuity projects
  - Fully redundant technical services outside of Los Angeles
  - Re-provision all services on fully redundant hardware, with well managed, scalable instances
    - Implementation of virtualisation etc.
    - Phase out last remaining legacy applications and services
  - Security auditing
- Focus on robustness and availability
- Much of this cost is not IANA-specific
  - IT department; L root expenses; etc.

Actual changes to IANA

- Three additional staff
  - Anticipate increase in work associated with new TLDs
- New automation development
  - Final work on deploying RZM solutions
  - Automation in other facets (e.g. protocol registries)
- DNSSEC
- Increasing costs of travel, etc.
- Anticipated actual “IANA” costs: 1.7m→2.5m (+50%)



Stolen from our CFO's slide deck

- Daily Operations cost is only nominally increasing

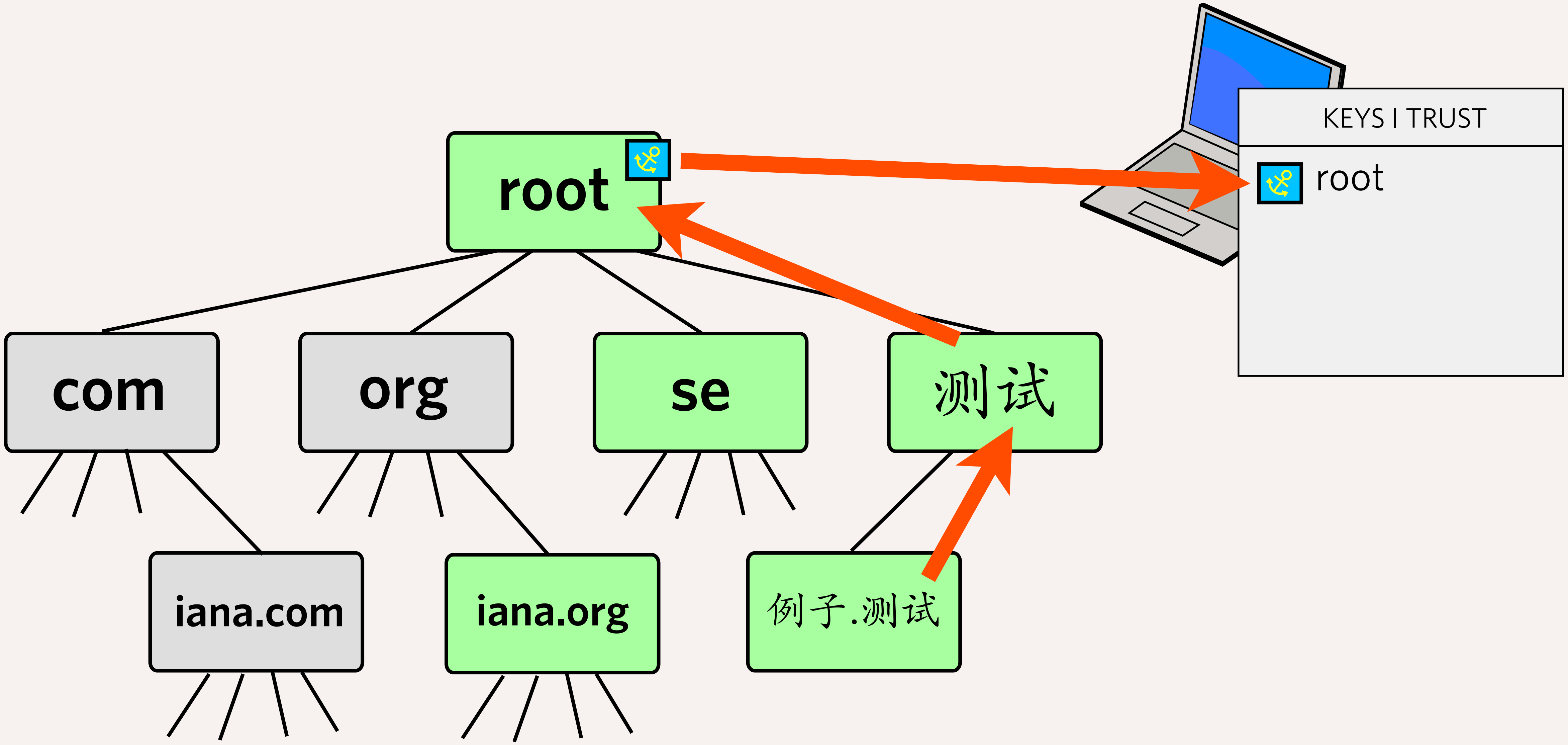
Comments welcome

- Draft Operating Plan and Budget for Fiscal Year 2009
  - http://tinyurl.com/4p3koo
- Presentation to ccTLD Managers yesterday
  - http://www.ccnso.icann.org/calendar/
- Comments can be lodged online, and are encouraged

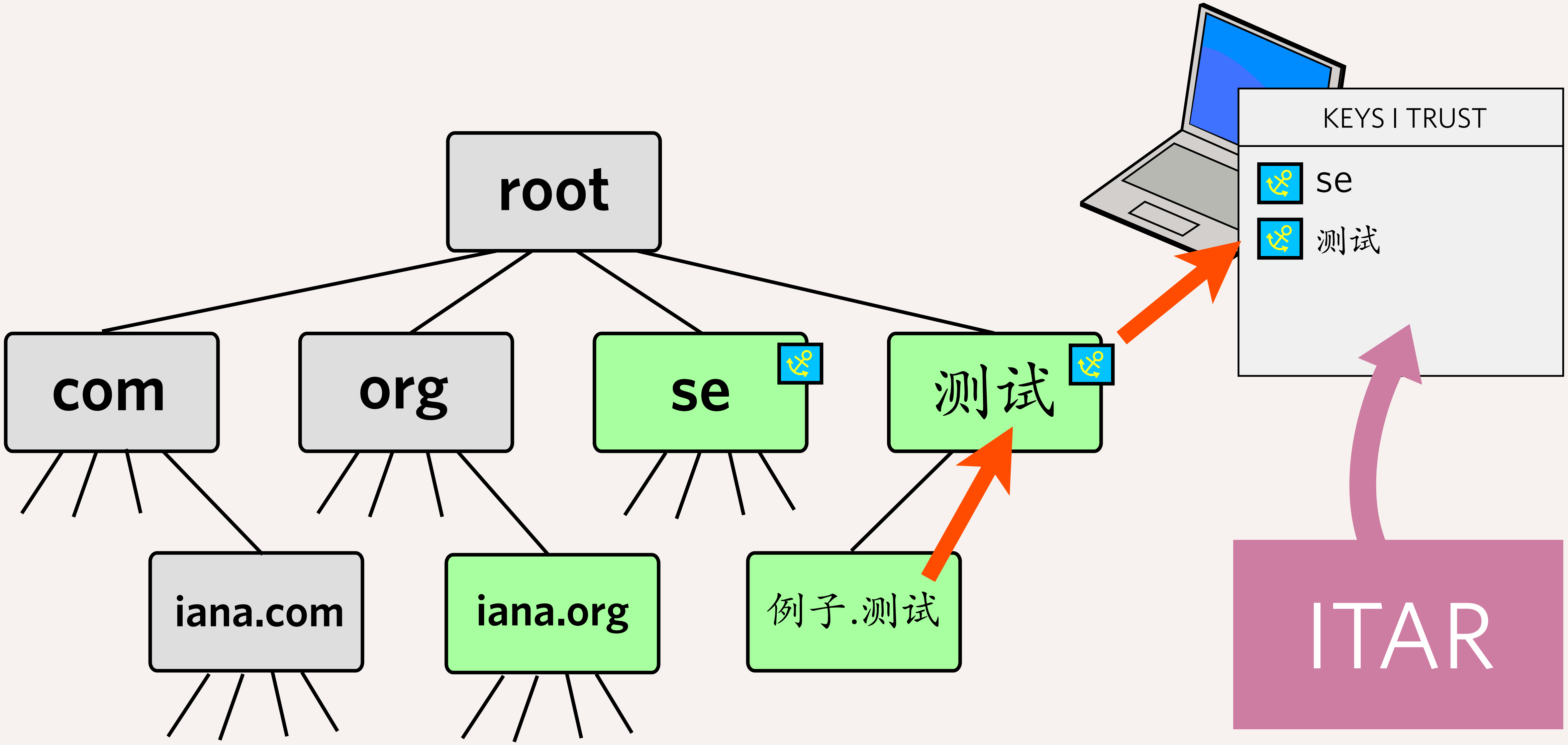
Interim Trust Anchor Repository

What is the ITAR?

- Interim Trust Anchor Repository
- A mechanism to publish keys of top-level domains that currently implement DNSSEC
- If the root zone is DNSSEC signed, such a repository is unnecessary
  - Therefore this is a stopgap measure
  - Should be decommissioned when the root is signed
- ICANN Board voted to implement in April 2008, based on community requests



If the root was signed



It isn’t so there are multiple trust apexes

RIPE Recommendations

1. Different “flavours” of TAs should be supported
2. Implementation neutral, supports common name servers
3. Verify key material is consistent and formatted correctly; Should have secure channel for authenticating requests
4. Process needed to revoke trust anchor, notify users of revocation.
5. Clear declaration of what “support” is available
6. Published exit strategy
7. Keys only published with consent of TLD operator

Supported Algorithms

- DNSSEC Key Algorithm
  - RSA/SHA-1 (type 5, see RFC 3110)
  - theoretically, algorithm neutral implementation
- DS Record Digest Types
  - SHA-1 (type 1, see RFC 4034)
  - SHA-256 (type 2, see RFC 4509)

Publishing formats

- Publication formats
  - List on website
  - XML structured format
  - Master file format
- Should work with major software implementations
- Formats are plain text and readable so implementors can modify to suit
- Implementors should not be putting special ITAR provisions in code — this is meant to go away when the root is signed!

Acceptance Model

- TLD operator can submit DS key data via web form
  - DS record validated against DNSKEY data in the DNS
    - Must match before the DS key is made active in the registry.
    - DNSKEY does not need to be in the DNS at time of submission (to allow for pre-deployment), but needs to validate prior to publication.
  - Administrative and Technical contacts for the domain must consent to the listing

Removal Model

- Identical to acceptance model, without the technical test
- List of revoked trust anchors will be provided

Exit Strategy

- ITAR will be decommissioned within x days of the DNS root being signed.

Limitations

- The ITAR will only operate for top-level domains
  - i.e. the keying information that would otherwise go in the root.
  - IANA will not accept anchors for descendants of top-level domains
    - Even if the relevant TLD is not signed

Implementation of RZM Software

Summary

- To implement software changes will require a contract amendment
- Key personnel changes at US Department of Commerce
- New process for implementation is being developed based on new requirements from USDOC
- Working with VeriSign in developing a concrete transfer proposal to obtain approval
    - VeriSign’s scope is limited to changing the implementation phase to a customised EPP-based workflow

Root Server “Hijacking”

Renumbering of the L Root Server

- 198.32.0.0/16 is a block set aside for Internet Peering Points ("Exchange Points"). It was previously listed in the ARIN database as "Exchange Point Blocks", but now to "EP.NET LLC".

- For historical reasons, "L" root service was placed in this block amongst another allocations for peering points. (Prior to ICANN's existence)

- As part of moving "L" out of the USC-ISI building, ICANN obtained a new net block and IP address for the service.

Renumbering (2)

- In liaison with the community and RSSAC, “L” was moved to the new IP address on 1 November 2007. ICANN undertook to continue service on the old IP address for a minimum of six months.
- Six months later, on 2 May 2008, ICANN discontinued service.
- The IP address kept responding to queries, surprising much of the Internet community.
  - The data being served was still “correct”.

What happened?

- EP.NET LLC entered into agreement with Community DNS to provide root service on the old L root IP address.
- ICANN was not informed of this, nor were the root operators, nor the community.
- Whilst arguably within rights to delegate service in such a way, we believe it was not in the interests to take this action.

Lessons to be learnt

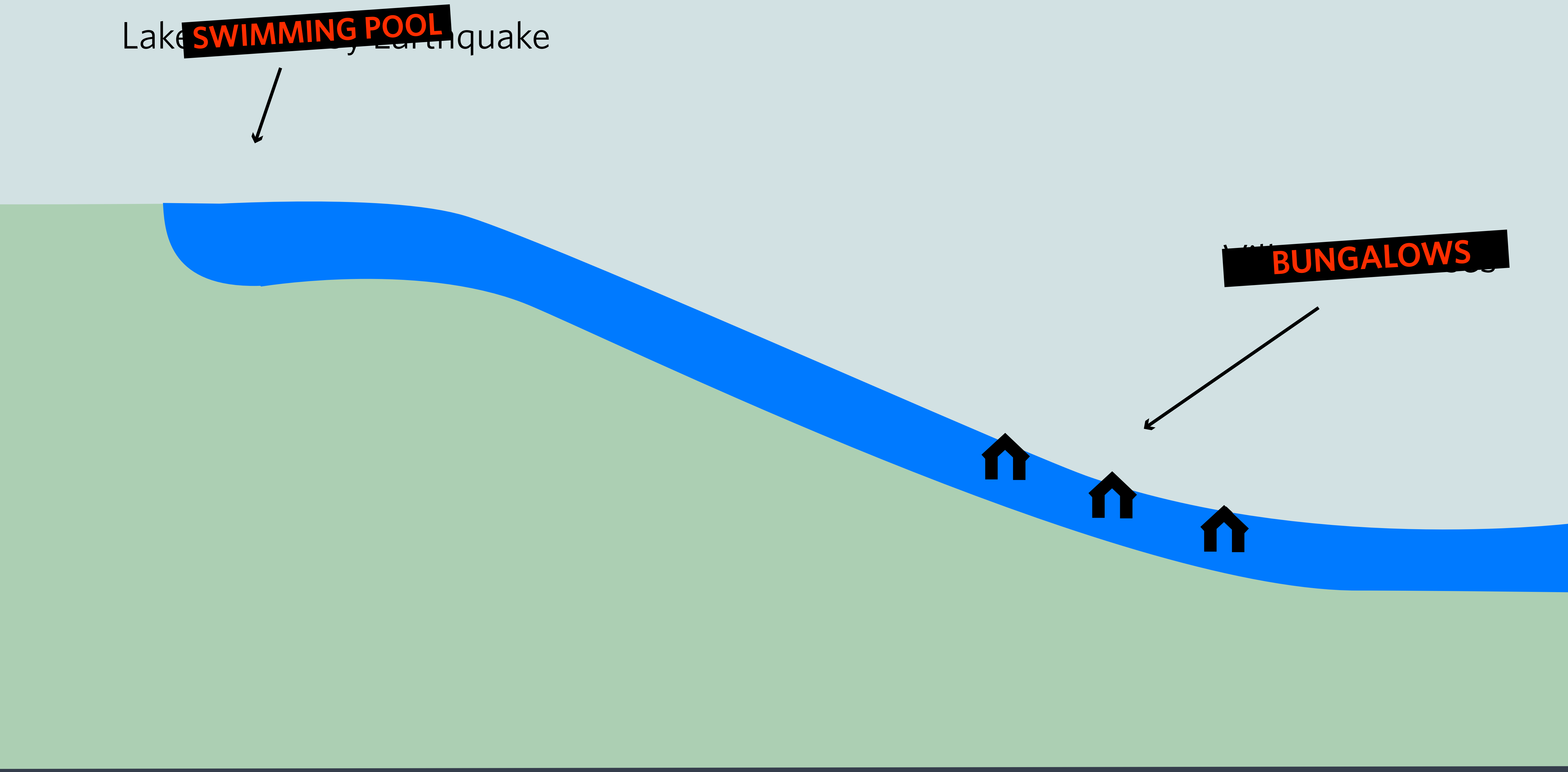
- This could not have been solved with rPKI (secure Internet routing technology), as the chain of custody for the IP address was ‘correct’.
    - So this is different from, say, the YouTube issue earlier this year.
        - Although, in an rPKI world, ICANN may have retained the more specific (/24) block delegated from the EP block.
    - However, a rogue party could do the same today with bad root data
- The EP.NET “L” was outside the coordination and management of ICANN, and unknown to the root server operator community.
- Highlights issues unique to the root servers, as their IP addresses are hard-coded in many places. Is the current IP address model for root servers correct?
- It is rather disappointing that the community was not engaged, nor was clear notice provided of the intent to continue service.

More discussion

- http://blog.icann.org/?p=309

Final Thought

Quake lakes



When things are too top-heavy...

New gTLDs

- 100? 1,000? 10,000?
- .google?
- Flattening of the DNS into the root zone?
- Doom?

Σας ευχαριστώ πολύ!

kim.davies@icann.org